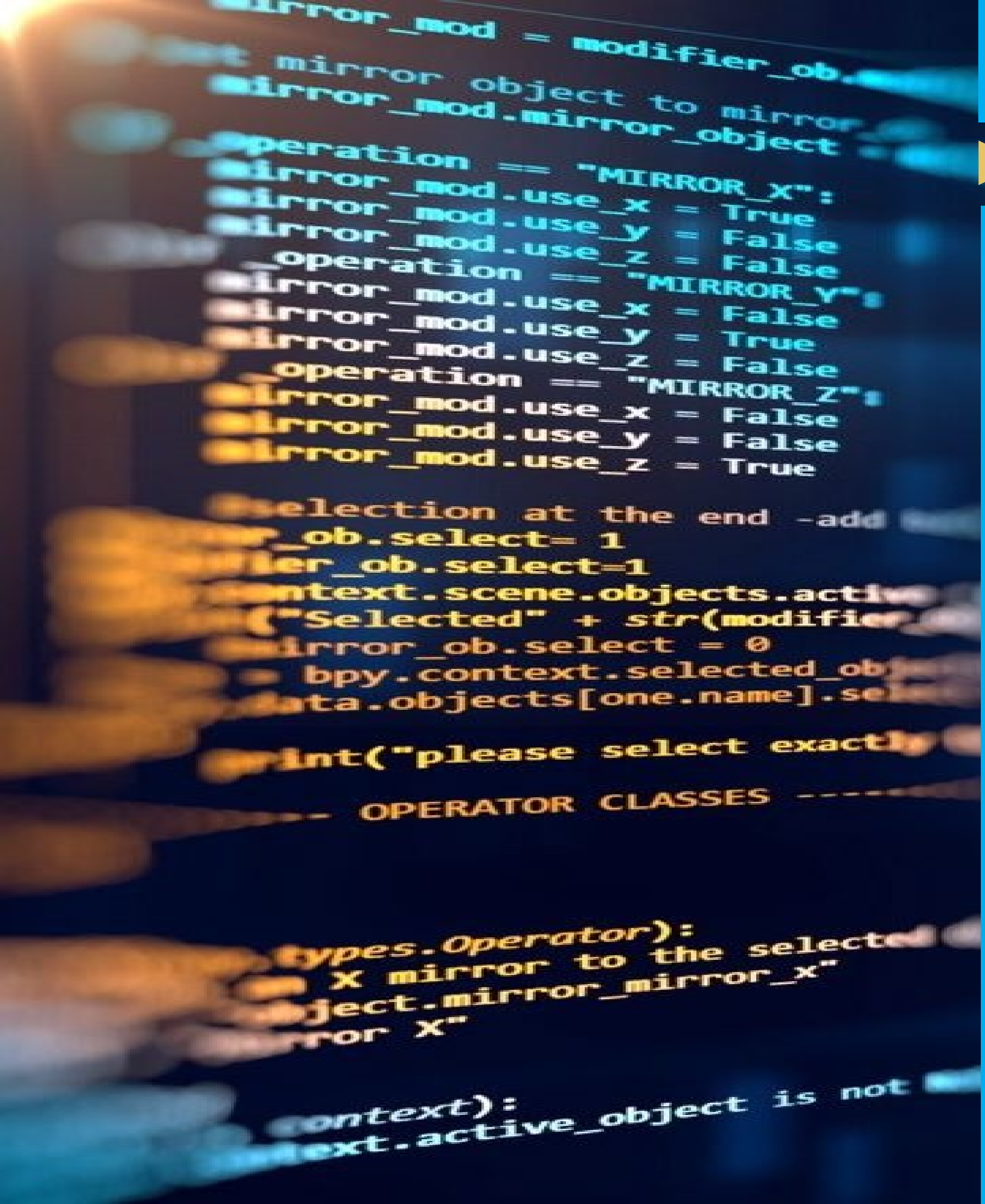


AN OFFERING IN THE BLUE CYBER SERIES

The Problem is Us!
Mitigating the PEBCAC

By Justin Frid

DoD Cyber Crime Center

26 September 2023

BLUE CYBER EDUCATION SERIES

DoD Cyber Crime Center

A Federal Cyber Center

The Problem is US! Mitigating the PEBKAC

Justin Frid
Cyber Analyst

31 May 2022

Agenda

- What is a PEBKAC?
- What is Social Engineering?
- Famous Examples
- Digital vs. Physical Social Engineering
- The Insider Threat
- The Psychological Attack Vectors
- The Five Aspects of Social Engineering
- Mitigation
- Questions

What is a PEBKAC?

P - Problem

E - Exists

B - Between

K - Keyboard

A - And

C - Chair

What is Social Engineering?

- **Social Engineering:**
  - **“The act of deceiving an individual into revealing sensitive information, obtaining unauthorized access, or committing fraud by associating with the individual to gain confidence and trust.”**

– NIST SP 800-63-3

- **Let us go up a “layer”:**
  - **“The psychological manipulation of human behavior that makes people act in certain ways by exploiting our cognitive biases and basic instincts.”**

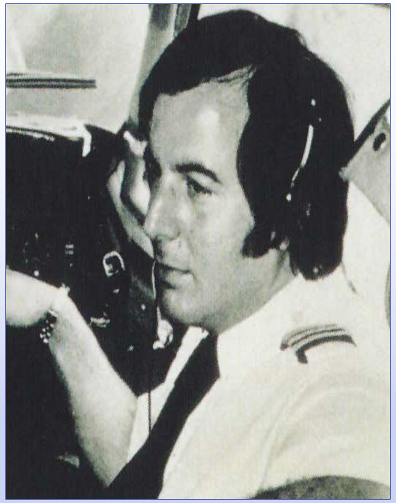
– Dr. Robert Cialdini

Famous Examples of Social Engineering

Kevin Mitnick

- "People, as I had learned at a very young age, are just too trusting."
- Charged in 1995 with 14 counts of Wire Fraud, 8 counts of Possession of Unauthorized Access Devices, Interception of Wire or Electronic Communications, Unauthorized Access to a Federal Computer, and Causing Damage to a Computer

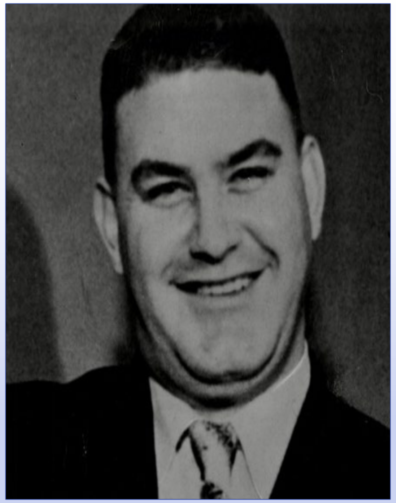
Famous Examples of Social Engineering



Frank Abagnale Jr.

- **"What I did in my youth is hundreds of times easier today. Technology breeds crime."**
- **Convicted on 8 charges out of 800 possible charges: seven counts of fraud, and one count for escape. Twelve countries sought his extradition for fraud**

Famous Examples of Social Engineering



Ferdinand “Waldo” Demara

- “… In any organization, there is always a lot of loose, unused power lying about which can be picked up without alienating anyone…”
- Impersonated a teacher, psychologist, editor, surgeon, engineer, and even a monk

Digital vs. Physical Social Engineering

Digital	Physical
Phishing	“Piggybacking” or Tailgating
Vishing	Impersonation
Social Media	Bribery/Quid Pro Quo
Watering Hole	Honeypot
Digital Media	Physical Media

So Where Does The Insider Threat Fit?

- Insider Threat:
  - "An entity with authorized access (i.e., within the security domain) that has the potential to harm an information system or enterprise through destruction, disclosure, modification of data, and/or denial of service."

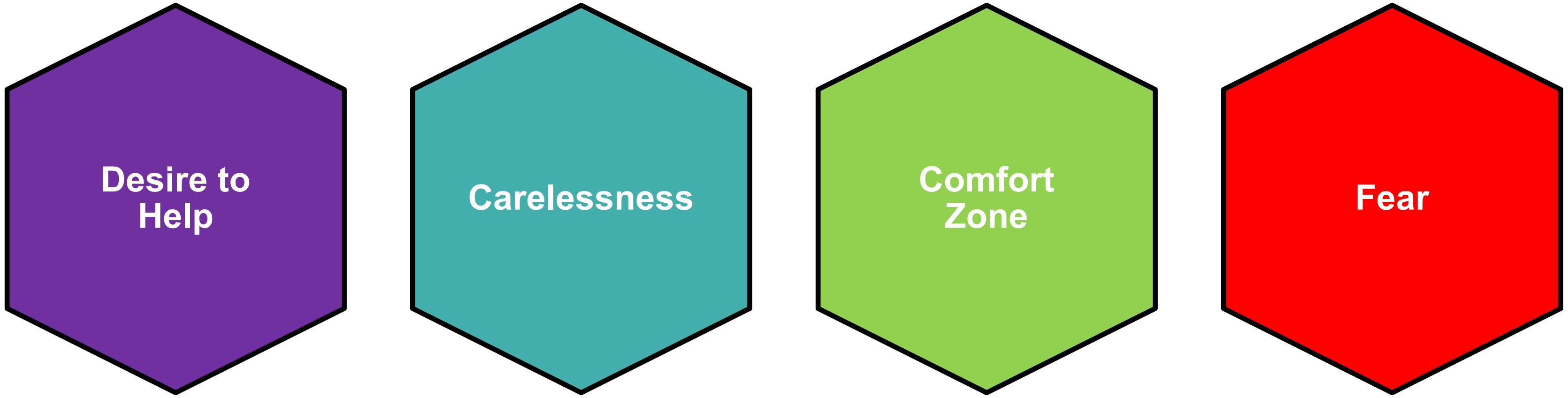
    – NIST SP 800-53 Rev. 4

- How are Social Engineering and Insider Threat related?
  - Accessing confidential data that is not relevant to the user's role
  - Attempts to access restricted areas
  - Requests for higher-level access without need
  - Irresponsible social media behaviors
  - Attempts to bypass security controls

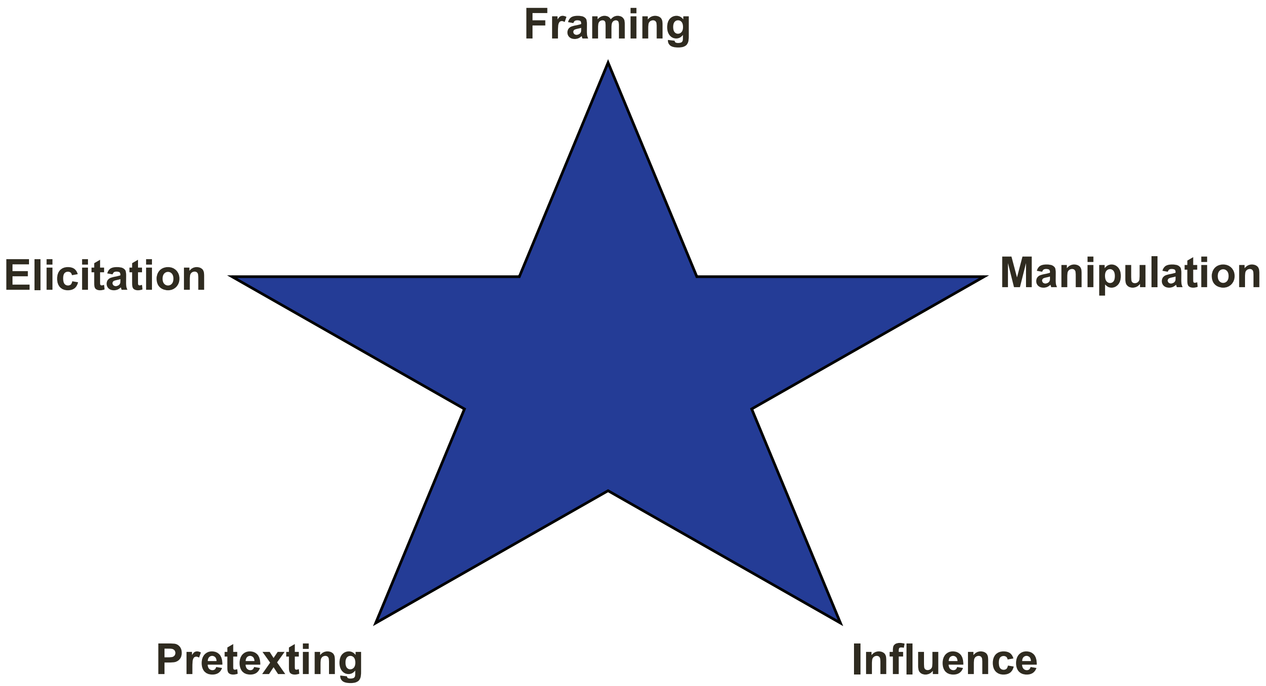
Insider Threat Cont.

- "Who do I report to if I've been the victim of or suspect an Insider Threat?"
  - If your organization suspects an Insider Threat, specifically relating to the unauthorized disclosure of Covered Defense Information (CDI), report the incident to your Facility Security Officer (FSO), who will, in turn, report it to your company's Defense Security Service Industrial Security Representative (DSS IS Rep)
  - Unauthorized Disclosures can be e-mailed to the DITMAC (DoD Insider Threat Management and Analysis Center) Unauthorized Disclosure Program Management Office (UD PMO) via group accounts:
    - SIPR: dss.quantico.dss-hq.mbx.ditmac-unauthorized-disclosure@mail.smil.mil
    - JWICS: DITMAC.UD@dss.ic.gov

Psychological Attack Vectors



The Five Aspects of Social Engineering



Framing

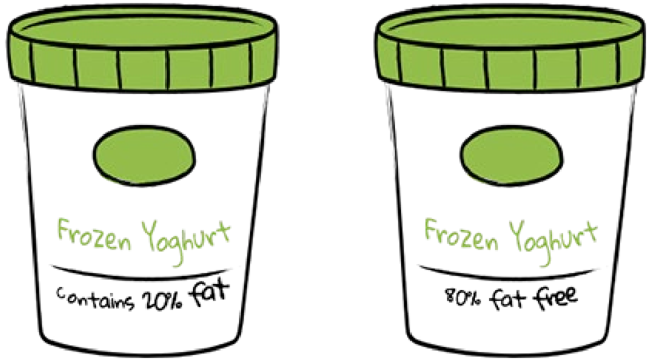
- **Framing:**
  - **"Framing is the act of forcing information into a certain context."**

    – Dr. Robert Cialdini

  - **Each individual has a series of psychological filters formed by their cognitive biases and cultural influences that, in turn, influences their perceptions of the world**

What's an example of Framing?

- **Consider the difference:**
  - **"The glass is half full!"**
  - **"The glass is half empty!"**



Elicitation

- Elicitation:
  - "A technique that strategically uses casual conversation to extract information from people (targets) without giving them the feeling that they are being interrogated or pressed for the information."

    – FBI Definition of Elicitation

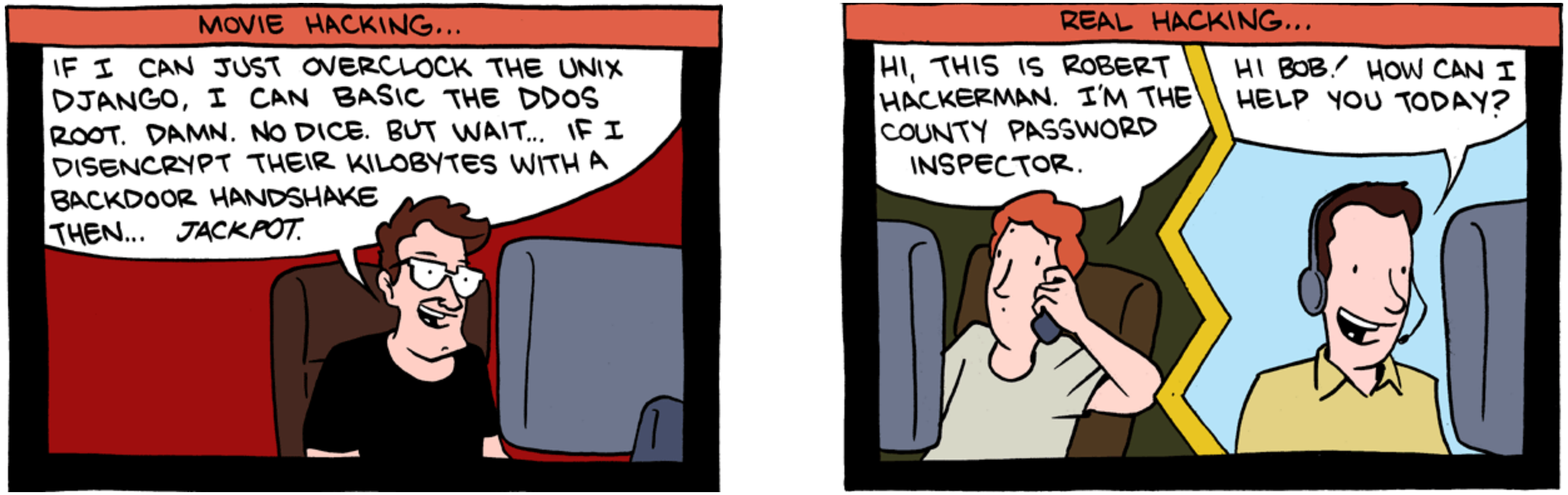
Common Tactics, Techniques, and Procedures of Elicitation:

- Flattery
- "Preloading"
- False Statements
- Feigned Ignorance

Pretexting

- **Pretexting:**
  - “The practice of presenting oneself as someone else in order to obtain private information.”

– Merriam-Webster


MOVIE HACKING...
IF I CAN JUST OVERCLOCK THE UNIX DJANGO, I CAN BASIC THE DDOS ROOT. DAMN. NO DICE. BUT WAIT... IF I DISENCRYPT THEIR KILOBYTES WITH A BACKDOOR HANDSHAKE THEN... JACKPOT.
REAL HACKING...
HI, THIS IS ROBERT HACKERMAN. I'M THE COUNTY PASSWORD INSPECTOR.
HI BOB! HOW CAN I HELP YOU TODAY?

Influence

The Eight Tactics of Influence in Social Engineering

Authority	Commitment and Consistency	Concession	Liking
Obligation	Reciprocation	Scarcity	Social Proof

Manipulation

- "Influencing and Manipulation are the same thing, right?"
  - Not necessarily. Influence is more about making people see your perspectives or fall more in line with your way of thinking. In contrast, Manipulation relies on coercion to forcibly bring someone in line with your way of thinking.
- Think of the difference between…
  - A car commercial that tells you that the brand is one of the most trusted in America, and is offering you bonus cash and 0% financing for a limited time
  - A car salesman who keeps going back and forth between you and their manager to consistently wheedle you into making a purchase today

Social Engineering Mitigation

- So how do we mitigate Social Engineering?
  - There is no substitute for TRAINING your users through an annual or semi-annual Security Awareness Training
  - Implement controls, such as spam filters or e-mail quarantines, to prevent attempts from reaching users
  - Ensure that your users understand the importance of privacy settings for their social media presence
  - Establish a clear working process for users to report suspicious activity either inside or outside of their workspace to your security detail
  - Implement physical controls, such as mantraps or badging systems, to limit physical access to only those who need it as part of their day-to-day duties

Insider Threat Mitigation

- How do we mitigate the Insider Threat?
  - As with regular Social Engineering: there is no substitute for <u>TRAINING</u> your users through an annual or semi-annual Security Awareness Training
  - Use resources, such as DSS's CDSE, to establish an Insider Threat Program to detect and respond to potential Insider Threat activity
  - Maintain audit logs of file transfer activity on your network, as well as flags for unusual log in times
  - Know and protect your critical assets while clearly documenting and consistently enforcing policies and controls

Summary

- Users are the most vulnerable part of any enterprise environment
- Real life examples of how devastating Social Engineering can be
- Social Engineering forms the backbone of many cyber intrusion vectors
- Understanding the psychological vectors on how users get leveraged
- We understand the Insider Threat and who to report to
- The Five Aspects of Social Engineering and how they apply to both real-life and cyber situations
- The importance of TRAINING through an established Security Awareness Training program

Resources

- Center for Development of Security Excellence
  - https://www.cdse.edu/
- DoD Insider Threat Management and Analysis Center
  - https://www.dss.mil/ma/tw/dvd/ditmac/
- NIST SP 800-50 Building an IT Security Awareness Training Program
  - https://csrc.nist.gov/pubs/sp/800/50/final
- The Social Engineering Framework
  - https://www.social-engineer.org/framework/general-discussion/